Raytheon
BBN Technologies

BBN Technologies
10 Moulton Street
Cambridge, MA 02138

25 July 2014

Office of Naval Research
875 North Randolph Street, Suite 1179
Arlington, VA 22203-1995

Delivered via Email to:
carey.schwartz@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil
shannon.viverette@navy.mil

Contract Number:	N00014-14-C-0002
Proposal Number:	P13003-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Jonathan Habif
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)
Contract Period of Performance:	7 February 2014 – 7 February 2016
Total Contract Amount:	$475,359 (Base)
Amount of Incremental Funds:	$205,668
Total Amount Expended (thru 11 April):	$89,748

Attention: Dr. Carey Schwartz
Subject: Quarterly Progress Report
Reference: Exhibit A, CDRLs

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its Quarterly Progress Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Habif at 617.873.5890 (email: jhabif@bbn.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kcarson@bbn.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson
Program Manager
Quantum Information Processing

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
25 JUL 2014		**07-02-2014 to 07-02-2016**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Raytheon BBN Technologies,10 Moulton Street,Cambridge,MA,02138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

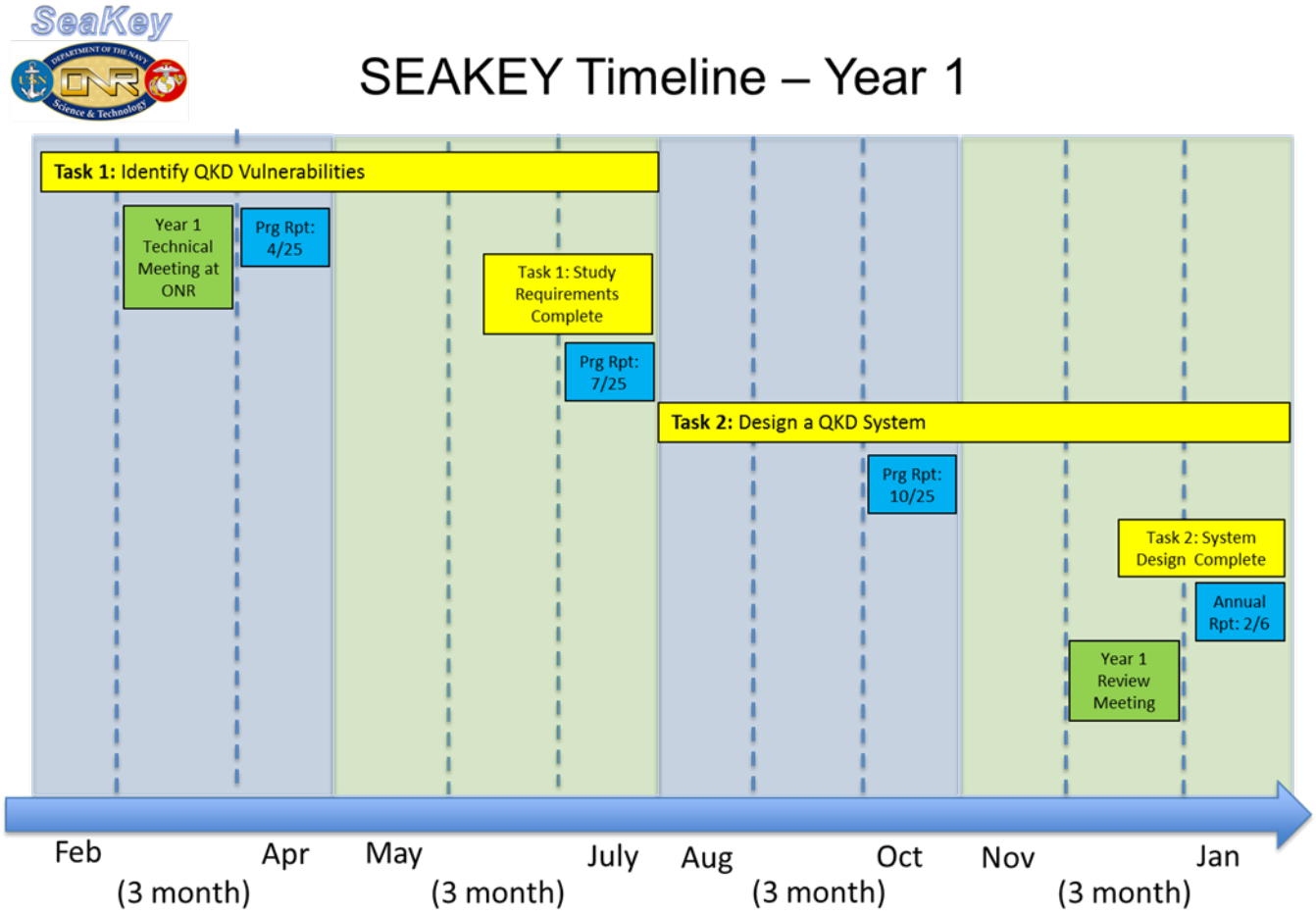
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**11**	

SEAKEY Quarterly Progress Report for the Period 26 April 2014 – 25 July 2014

Section A. Project Schedule

The Year 1 timeline below identifies SeaKey tasks, their duration, task milestones, kickoff meeting, tentative program review meeting, and progress report due dates.



Section B. Technical Progress

SUMMARY

In this report we summarize the technical progress accomplished during the second quarter of work of the SeaKey program encompassing the first half year of work on the program. We describe our information theoretic work to define the performance bounds of QKD systems operating under ideal scenarios, and how those bounds guide our path forward for link design. We also describe our progress quantifying the non-idealities

that will be encountered in a free-space optical (FSO) link operating in a marine environment.

INTRODUCTION

Our work, to date, has spanned two major efforts: (1) continuing to determine the non-idealities that will be encountered operating an optical communications link in a free-space channel through a marine environment (such as loss, noise and turbulence) and (2) parametrically calculating the secret key rate that can be expected.

RESULTS AND DISCUSSION

Nonidealities in the marine environment:

Our team has looked at various atmospheric nonidealities, including the effects of (1) atmospheric absorption, (2) aerosols, (3) water vapor, (4) turbulence-induced amplitude and phase fluctuations, on loss, and that of the blackbody and sky radiance on detector background counts. We also examined the effects of detection nonidealities, such as detection inefficiency and dark clicks. The main objective was to zero in on a few candidate windows of operation.

The investigation of atmospheric nonidealities was done by RVS, using MODTRAN. A few different environments (mid-latitude summer, tropical) and ranges from 1-10 km were considered.

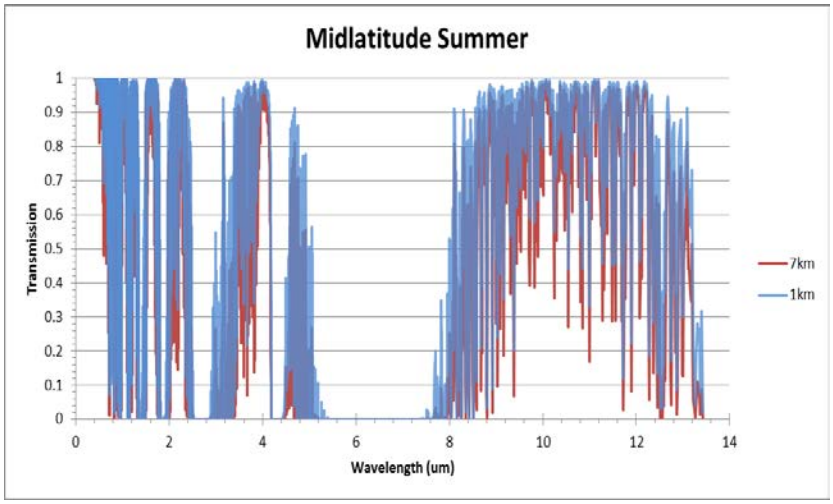


Fig. 1: Atmospheric transmission in a midlatitude summer environment, in the presence of no aerosol

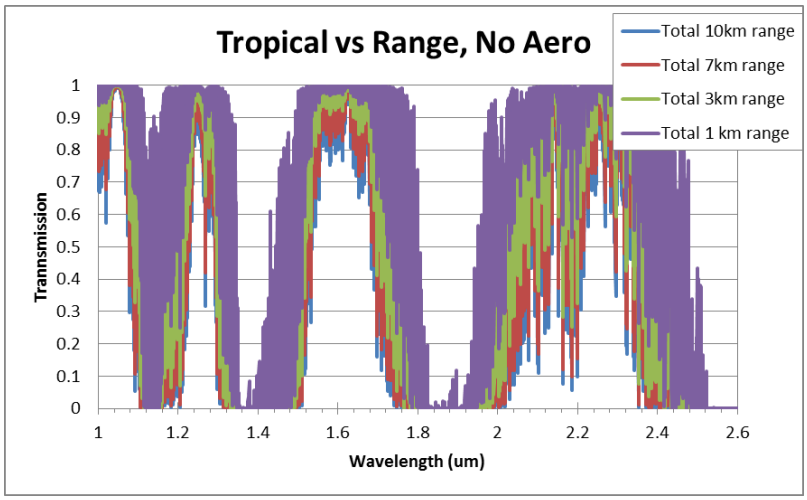


Fig. 2: Atmospheric transmission in a tropical environment, in the presence of no aerosol

As can be seen from figures 3 and 4, there is a net decrease of atmospheric transmission when one considers the effect of aerosol absorption and water vapor continuum.

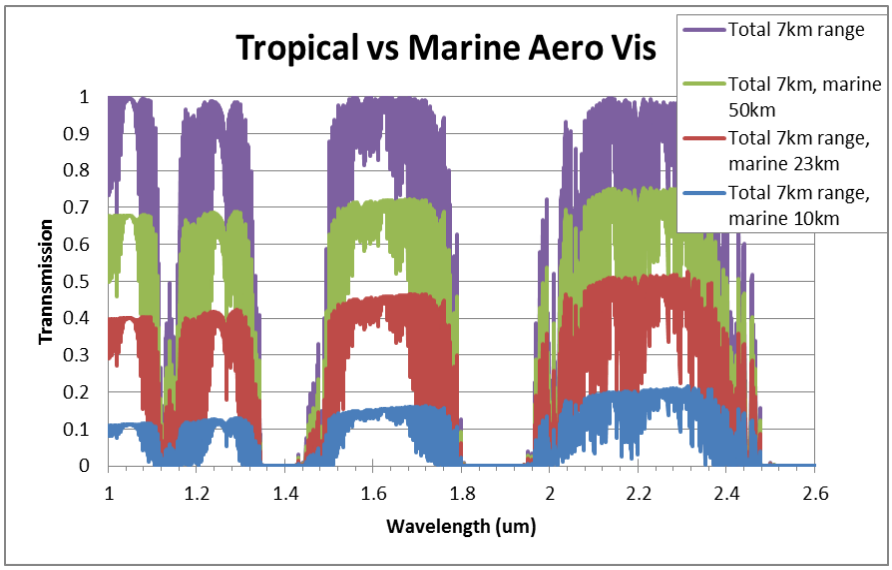


Figure 3: Marine atmospheric transmission data in the presence of aerosol for a range of 7 km, and a few candidate visibilities (10 km, 23 km and 50 km).

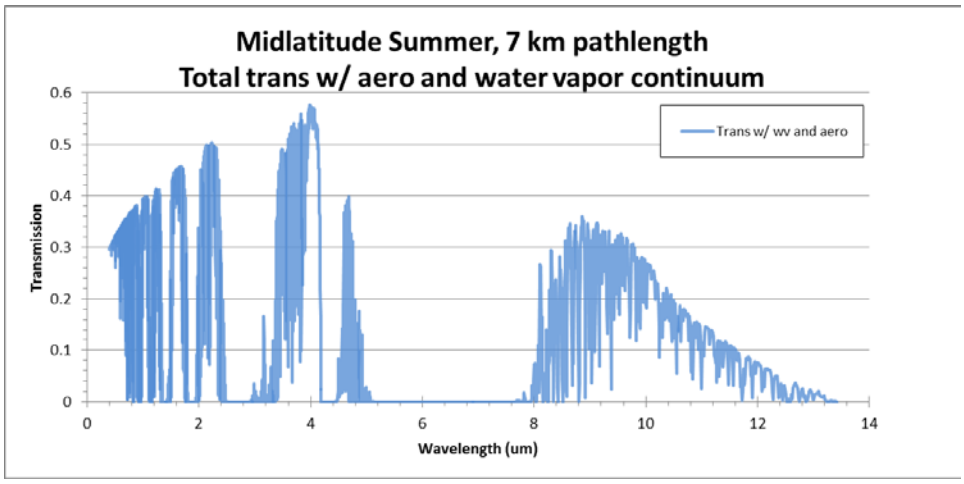


Figure 4: Atmospheric transmission over a 7 km pathlength, in the presence of water vapor and aerosol absorption.

Looking at the trade-off between blackbody radiance, sky radiance and atmospheric transmission, the three candidate wavelengths we identified are 1.5 μm, 2.2 μm and 4μm (see figure 5). Of 2.2 μm and 4 μm, former has worse (higher) loss, but better (lower) noise. Even though quantum cascade lasers operate in the deep infrared, a potential roadblock in operation above 4 μm is the lack of availability of low-noise, high-efficiency single-photon detectors.

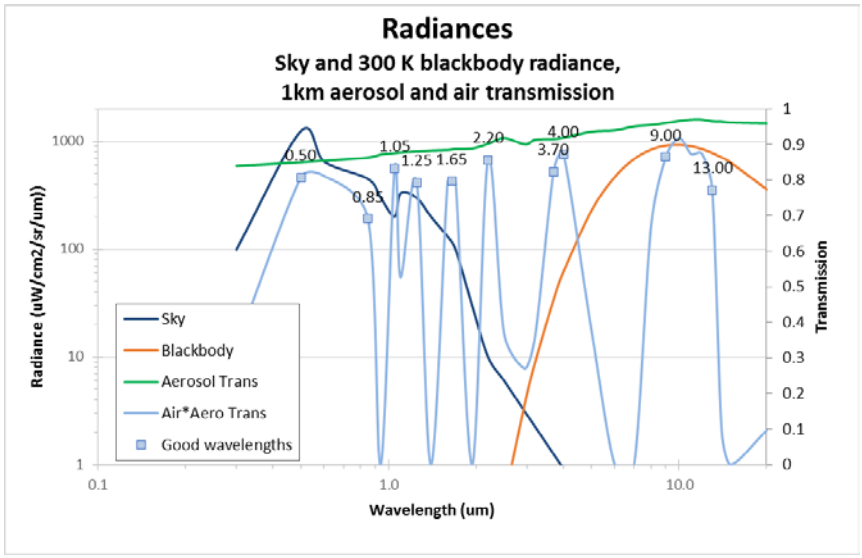


Figure 5: Wavelength dependence of sky radiance, blackbody radiance, aerosol and air transmission.

For blackbody and sky radiance, we estimated the following dependence of detector background counts on wavelength, assuming that the receiver aperture has 10 cm radius, 5 arc seconds field of view and 1 pm spectral filter width.

Wavelength	**Blackbody radiance** ($W\ m^{-2}\ sr^{-1}\ \mu m^{-1}$)	**Sky radiance** ($W\ m^{-2}\ sr^{-1}\ \mu m^{-1}$)	**Background counts/sec due to blackbody radiance**	**Background counts/sec due to sky radiance**
1550 nm	0.000000566	1.5	6.4E-05	169.6
2200 nm	0.000839	0.2	0.2	32.3
4000 nm	0.7373	0.009	215.1	2.6

Parametric calculations of the expected secret key rate

As can be seen in Figure 6, the secret key rate of the BB84 protocol in the presence of these nonidealities is very similar across the wavelength ranges of interest.

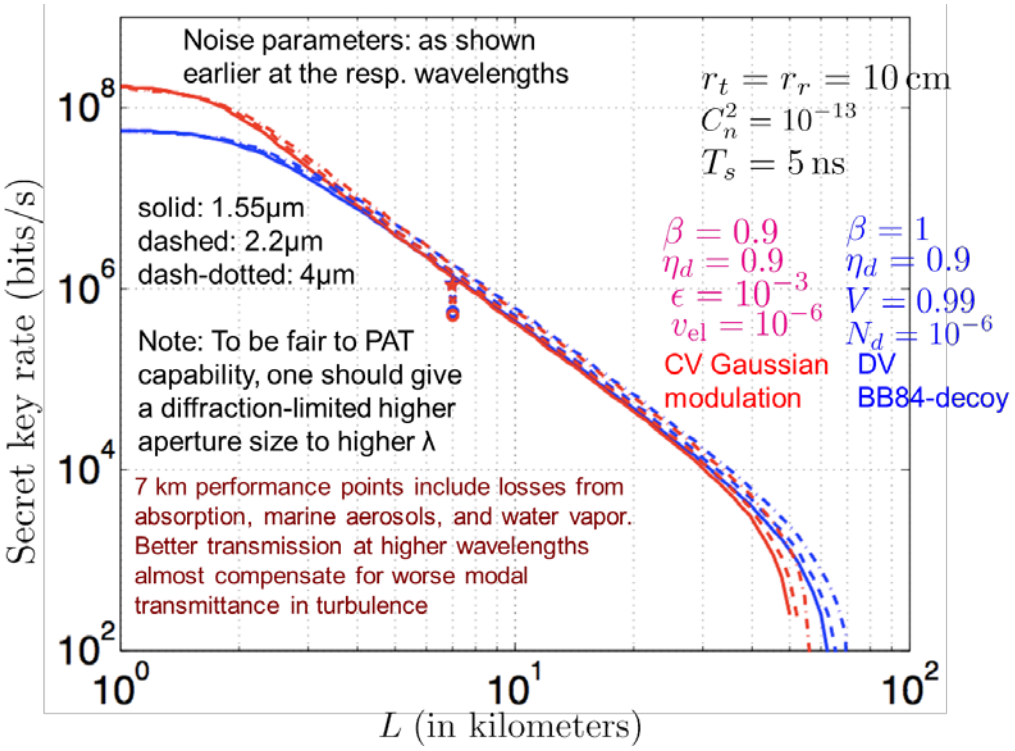


Figure 6: Secret key rate of the DV BB84-decoy and CV Gaussian modulation protocols as a function of wavelength .

Figure 7 shows an analysis of how secret key rate for different protocols (such as CV-BPSK, DV-BB84 and the like) scales with loss.

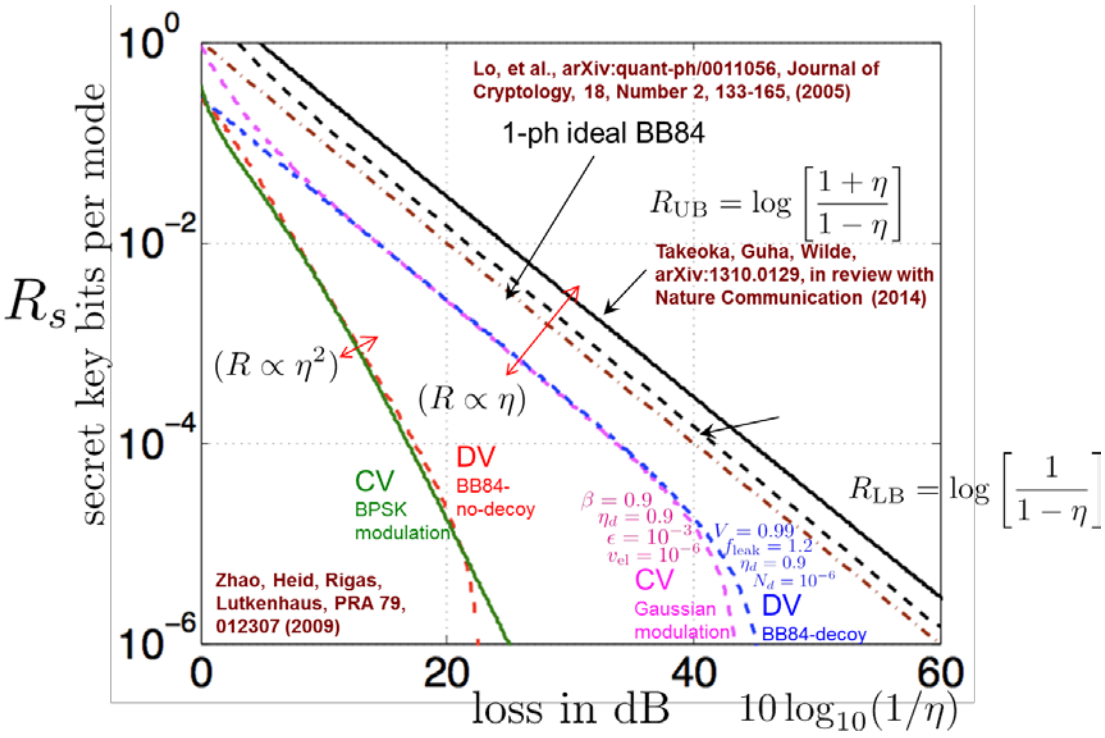


Figure 7: Key rate vs loss

We have identified a rate upper-bound, $R_{UB} = \log_2[(1+\eta)/(1-\eta)]$ bits/mode, which defines the maximum rate at which secret-key generation (QKD), entanglement generation and quantum communication (each with reverse public classical channel) channels can operate. This rate upper bound applies to all protocols, including high-dimensional QKD. As can be seen from Figure 7, BB84 is already very close to the upper bound. If the detector is bandwidth-limited, high-dimensional coding could be beneficial. But otherwise, decoy-state BB84 might suffice.

Figure 8 shows the performance of QKD protocols vs direct secure communication protocols. The direct-secure communication protocol achieves optimum scaling.

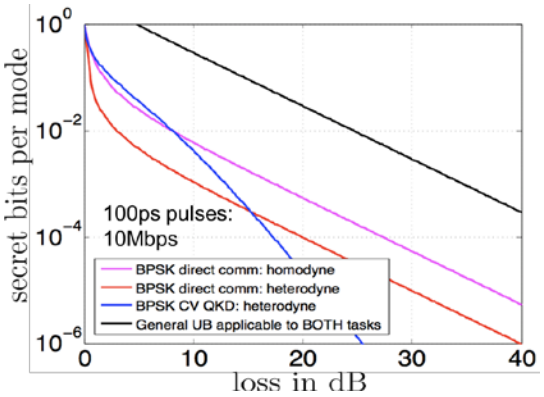


Figure 8: QKD vs direct secure communication

Figure 9 shows the effect of various detriments on the secret-kay rate, for laser-decoy BB84.

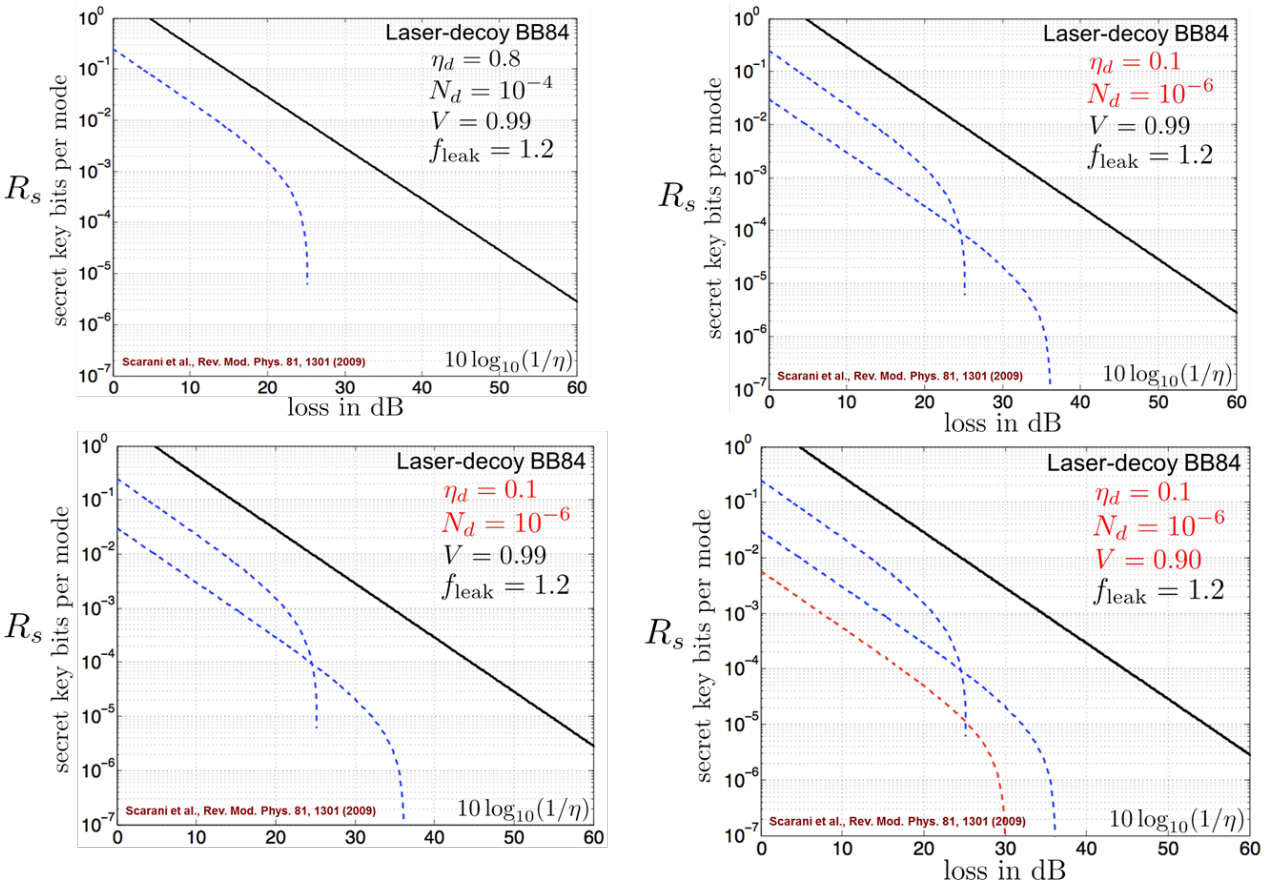


Figure 9: Effects of detriments on secret-key rate

We also examined the performance of a single-mode Gaussian beam in a turbulent channel (Figure 10), in order to estimate the secret key rate of the CV Gaussian Modulation and decoy-state BB84 protocols in the presence of turbulence (Figure 11).

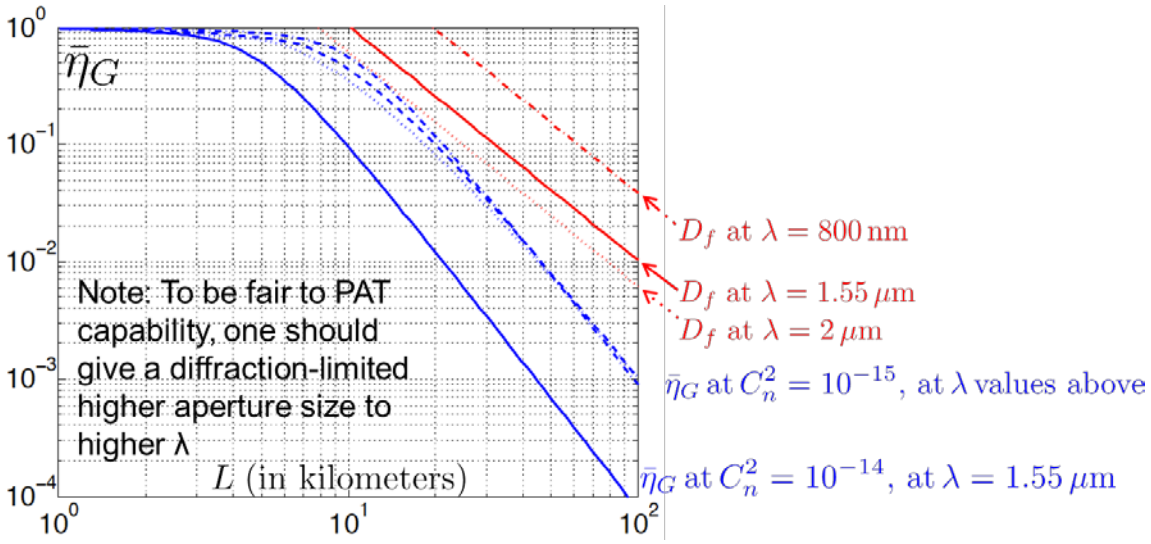


Figure 10: Mean transmittance of a focused Gaussian beam in a turbulent channel

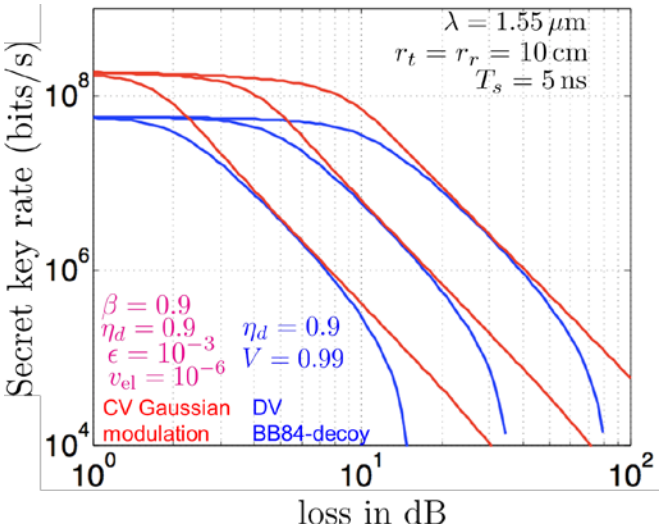


Figure 11: Secret key rates of the CV Gaussian modulation and DV BB84 decoy-state protocols in the presence of turbulence

Section C. Problem Areas – Identification

There are no anticipated problems or issues to report at this time.

Section D. SEAKEY Financial Update

Financial Chart reflecting Year 1: